BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-216

1 NOVEMBER 1997

Communications and Information

MANAGEMENT OF MANUAL CRYPTOSYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCI (Ms Jean Alf)
Certified by: HQ USAF/SCXX (Lt Col Webb)
Supersedes AFI 33-216, 1 October 1995.
Pages: 14
Distribution: F

This Air Force instruction (AFI) establishes objectives, assigns responsibility for ensuring maximum efficiency in the management of manual cryptosystems, and sets-up a program of periodic evaluations of manual cryptosystems to ensure the systems fulfill the operational and cryptographic security requirements of the users. This instruction applies to all controlling authorities, users of manual cryptosystems, Headquarters Cryptologic Systems Group (HQ CPSG/ZCK), and Headquarters Air Force Communications Agency (HQ AFCA/GCI). It implements National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 3014, *(FOUO) Management of Off-Line Cryptosystems*; National COMSEC/EMSEC Information Memorandum (NACSIM) 7001, (C) *COMSEC Planning Guide for Manual Cryptosystems (U)*; and Air Force Policy Directive (AFPD) 33-2, *Information Protection*. In-depth guidance on handling and using manual cryptosystems is in AFKAG-1, *Air Force Communications Security (COMSEC) Operations*; Air Force Systems Security Instruction [AFSSI] 4100, (C) *Communications Security Program (U)* (will convert to AFI 33-201); and AFI 33-211, *Communications Security (COMSEC) User Requirements*. Do not release this publication to the general public without specific approval from HQ AFCA/GCI. The term "major command" (MAJCOM), when used in this publication, includes field operating agencies and direct reporting units. Direct queries and recommended changes about this publication through appropriate MAJCOM channels to HQ AFCA/GCI, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234. Send messages to: HQ AFCA SCOTT AFB IL//GCI//. Refer conflicts between this and other instructions to HQ AFCA/XPXP, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5233, using AF Form 847, **Recommendation for Change**, with an information copy to Headquarters Air Force Communications and Information Center (HQ AFCIC/SYNI), 1250 Air Force Pentagon, Washington DC 20330-1250. Use the questions at **Attachment 2** and **Attachment 3**, and AF Form 2519, **All Purpose Checklist** (available electronically) to develop a checklist on manual cryptosystems. See **Attachment 1** for a glossary of references, abbreviations, acronyms, and terms.

SUMMARY OF REVISIONS

Updates unit designators and makes office symbol changes. A "|" indicates revision from previous edition.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01 Nov 1997	N/A	-

Title and Subtitle Air Force Instruction 33-216 Communications and Information Management of Manual Cryptosystems	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington D C 20330-1250	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 14	

1. Responsibilities:

1.1. National Security Agency (NSA). Conducts a continual assessment program to ensure the adequacy of system design and security and establishes minimum standards for revalidations and surveys.

1.2. HQ AFCA/GCI:

1.2.1. Provides assistance, as necessary, to controlling authorities and users in conducting and scheduling surveys.

1.2.2. Coordinates with HQ CPSG/ZCK on scheduling annual revalidations on the manual cryptosystems.

1.2.3. Provides the results of revalidations and surveys to the NSA.

1.3. HQ CPSG/ZCK:

1.3.1. Provides complete instructions on manual cryptosystem annual revalidations to controlling authorities.

1.3.2. Schedules annual revalidations in conjunction with the appropriate controlling authority.

1.3.3. Coordinates with HQ AFCA/GCI on the revalidations.

1.4. Controlling Authorities:

1.4.1. Are designated before approval of a new system for production. The organization appointed to fulfill controlling authority duties is normally included in the handling instructions for each system. The controlling authority is usually the highest-level organization in the operational network that uses the manual cryptosystem. AFI 33-215, *Controlling Authorities for COMSEC Keying Material*, prescribes the responsibilities of organizations that serve as controlling authorities for communications security (COMSEC) manual cryptosystems. The need to ensure close, positive supervision over applying and using these systems determines the requirement to appoint controlling authorities in the operational chain of command for each manual cryptosystem. Controlling authority responsibilities include:

1.4.1.1. Administration:

1.4.1.1.1. Validates cryptonet members and the COMSEC accounts authorized to hold the manual cryptosystems.

1.4.1.1.2. Establishes the effective date for each edition of the manual cryptosystems and keeps all members of the cryptonet informed.

1.4.1.1.3. Specifies the key-change time for the cryptonet.

1.4.1.1.4. Recommends changes in the system design (for example, the content or format of the manual cryptosystems).

1.4.1.1.5. Makes spare group assignments in operation codes as necessary.

1.4.1.1.6. Authorizes local reproduction of manual cryptosystems when established cryptologistics channels cannot supply the material in time to meet urgent, unprogrammed, operational requirements.

1.4.1.1.7. Reports and evaluates security incidents concerning the manual cryptosystem according to AFI 33-212, *Reporting COMSEC Incidents*.

1.4.1.1.8. Conducts an annual revalidation to confirm that there is a continuing need to produce the manual cryptosystems in present quantity, and reports the results to HQ CPSG/ZCK, 230 Hall Boulevard, STE 112, San Antonio TX 78243-7056, who then forwards the results to Director of NSA (DIRNSA/V611) and HQ AFCA/GCI. **NOTE:** The reporting requirement in this paragraph is exempt from licensing in accordance with paragraph 2.11.1 of AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and InterAgency Air Force Information Collections* (will convert to AFI 33-324).

1.4.1.2. Logistics. Notify the distribution sources of any changes that could affect the distribution of manual cryptosystems.

2. Evaluation . Improvements in the quality of manual cryptosystems are a matter of continuing interest to both the producers and users of these systems. Revalidations and surveys are the principal source of information concerning the suitability of a manual cryptosystem in its operational environment. Feedback to and from the field using these methods allows early identification and improvement to existing manual cryptosystems. All controlling authorities must revalidate manual cryptosystems annually and conduct surveys as needed. As a minimum, revalidations will include the following:

2.1. Validate a continuing requirement for the manual cryptosystem.

2.2. Affirm that the cryptosystem design and content are adequate. If not, identify needed changes.

2.3. Certify that current distribution of the cryptosystem is correct. This includes verifying that present users have a continuing need for the system, that stock copies are adequate, and that any additional users are identified.

2.4. Identify ongoing or planned actions that might affect requirements for the system.

2.5. Revalidate one-time pads annually for security purposes. Responsible authorities designated in paragraph 1 may; however, require surveys of one-time pads as needed, to make sure the requirement still exists.

2.6. Use the checklist in **Attachment 3** to perform a survey.

3. General Information on Codes, Authentication Systems, and One-Time Pads.

3.1. Description of Cryptosystems. NSA produces manual cryptosystems and distributes them through COMSEC channels. Air Force organizations can get manual cryptosystems through the local base COMSEC manager. Manual cryptosystems consist of any cryptographic system that does not use electric or electronic principles to convert plain text to code or cipher text. The most common types of manual cryptosystems are codes, one-time pads, and authentication systems.

3.2. Production of Cryptosystems. Cryptosystems are produced by NSA or by HQ CPSG/ZCK when specifically authorized. Users process requests for new systems or changes in existing systems through command channels to HQ AFCA/GCI. HQ AFCA validates these requests and submits specifications to NSA. Do not send requests directly to NSA. Individual commands or other organizations subordinate to the MAJCOM will not develop, produce, or use manual cryptosystems that are not approved by NSA. Locally produced manual cryptosystems do not contain the cryptographic principles needed to guarantee the required amount of protection.

3.3. Obtaining and Requesting Assistance of Manual Cryptosystems Currently in Use:

3.3.1. AFI 33-211 requires the supporting COMSEC manager to submit requests according to AFKAG-2, *(FOUO) AF COMSEC Accounting Manual*.

3.3.2. If assistance is needed to determine system suitability or selection, or if the command desires other COMSEC advice on manual cryptosystems, send a letter or message to HQ AFCA/GCI. Include the following information:

3.3.2.1. Short title, long title, or type of system under consideration, if known.

3.3.2.2. Brief description of the planned use, type of information to secure, by whom, to whom, and amount of traffic estimated in a 24-hour period.

3.3.2.3. Classification of the data needed to encipher or secure using the system.

3.3.2.4. Project officer or office and telephone number.

3.4. Requesting New Code and Authentication Systems. Submit requests through command channels to HQ AFCA/GCI for evaluation and approval to maintain standards of security and provide the most appropriate system to meet a particular need. **Attachment 2** is a checklist designed to aid in describing requirements. Submit new requirements in the format provided by the checklist to reduce the time required to fulfill them and to assist in properly evaluating the capabilities of available systems. Make sure the project officer's name, office symbol, and telephone number are on the request.

3.4.1. COMSEC managers will publicize the existence of these procedures and the checklist to all activities having potential new code and authentication system requirements, pointing out the necessity of following these provisions when submitting new requirements.

3.5. Operations Code Training. COMSEC publication AFKAO-5, *(C) Instructional Guide for Operations Codes* (U), is available from the local base COMSEC managers and provides instructions for using operations codes, preparing messages for encoding, and applying related communications procedures.

4. Manual Cryptosystem Management Surveys. Management surveys provide the controlling authorities and production agencies with user-level operational statistics and specific recommendations for changes to system design, format, content, and suitability. HQ AFCA/GCI will coordinate with controlling authorities and NSA to conduct required surveys of Air Force controlled systems. However, if MAJCOMs or controlling authorities feel a survey is needed, they may conduct a survey at any time and send the results to HQ AFCA/GCI. Other services, or NSA/V611, may conduct management surveys for joint and allied manual cryptosystems. Applicable Air Force units must participate in these surveys.

4.1. Surveys. The management survey program is designed to determine the suitability of existing manual cryptosystems by gathering facts on usage rate, message volume, and ways of transmission. Surveys:

4.1.1. Request vocabulary, format, and composition changes.

4.1.2. Provide the most accurate way to estimate future quantitative requirements.

4.1.3. Promote a better understanding of the material's purpose by managers, controlling authorities, and actual users.

4.1.4. Determine actual user requirements, the extent of material usage, and if the material satisfies the operational need of the users.

4.1.5. Highlight deficiencies in the material and changes in supersession rate (based on current usage).

4.1.6. Identify if changes are anticipated in distribution (reductions or increases in quantities).

4.2. Types of Surveys. There are two major types of surveys:

4.2.1. Initial Survey. Each new manual cryptosystem is scheduled for survey approximately 90 days after the implementation date to determine:

4.2.1.1. If the system is fulfilling the requirement for which it was established.

4.2.1.2. Whether vocabulary or format changes are required.

4.2.1.3. If changes in quantitative requirements are required before developing a firm production schedule.

4.2.2. Periodic Survey. HQ AFCA/GCI will direct a periodic survey of a manual cryptosystem**:**

4.2.2.1. When requested by NSA, a MAJCOM, or controlling authority.

4.2.2.2. When the vocabulary is outdated or inadequate.

4.2.2.3. When copies issued have so decreased that the system's value is questioned.

4.2.2.4. When there is the possibility of combining systems.

4.2.2.5. When there is limited or increased use of the system.

4.2.2.6. When there is an increase or decrease in activities in any geographic area.

4.2.2.7. Following a change of command's mission.

4.2.2.8. To establish an accurate account of actual users.

4.2.2.9. When a comparison of user type is needed (for example, aircraft versus ground units).

4.2.2.10. When directive material has changed.

4.2.2.11. At least every four years.

4.3. Survey Procedures. When a management survey of a system is advisable, HQ AFCA/GCI will coordinate with the system's controlling authority to get approval and propose recommended survey dates. The survey will include particular areas that the controlling authority considers desirable. The controlling authority notifies all holders of the system of the impending survey. The controlling authority then conducts the survey and sends all survey results to HQ AFCA/GCI. It takes approximately 60-90 days to prepare the survey material, mail it to the applicable COMSEC accounts, and allow the COMSEC accounts time to send it to the users.

4.4. Survey Forms. AFCOMSEC Form 12, **COMSEC Code System Survey Report**, is used to record the data requested by management surveys. The COMSEC manager ensures that each issuing activity and actual user activity completes a copy as specified in the notification letter. Classify forms according to content. The issuing activities and actual users will return the completed form to the COMSEC manager within 5 days after the survey period closes, unless directed otherwise. **NOTE:** The reporting requirement in this paragraph is exempt from licensing according to paragraph 2.11.1 of AFI 37-124.

4.5. Final Report. HQ AFCA/GCI will revalidate information on the survey forms and prepare an analysis in report format. The final report will include, but is not limited to:

4.5.1. System description and method of application.

4.5.2. Number and percentage of COMSEC accounts participating in the survey.

4.5.3. Number of copies required for distribution.

4.5.4. Type of user facility.

4.5.5. Current system usage by percentage of total user facilities.

4.5.6. Number and type of messages encrypted in the system.

4.5.7. Transmission methods used.

4.5.8. Prescribing directives.

4.5.9. Proposed distribution and usage changes.

4.5.10. Users' comments.

4.5.11. Recommended changes in system vocabulary.

4.5.12. Other recommendations on managing the system from both the qualitative and quantitative viewpoints.

4.6. Processing Reports. HQ AFCA/GCI will prepare a report and send the report to the system controlling authority who approves or disapproves recommendations made in the report. HQ AFCA/GCI will then send the approved recommendations to NSA/V611 for further reporting to the production agency for action. NSA must approve any proposed changes in supersession rate.

4.6.1. Comments and recommendations. The Management Survey Program is not intended to restrict controlling authorities, COMSEC managers, or users from submitting comments.

4.6.1.1. User recommendations are encouraged, especially changes to the vocabulary, to keep it current with day-to-day operations and weapons systems used.

4.6.1.2. COMSEC manager recommendations are also emphasized, particularly on handling procedures, between the manager, issuing activity, and actual system user.

4.6.2. Reporting channels. Report comments and recommendations on COMSEC matters through command COMSEC channels. COMSEC managers are encouraged to assist users in formulating their comments and recommendations into standard COMSEC phraseology.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

AFPD 33-2, *Information Protection*

AFI 31-401, *Managing the Information Security Program*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Incidents*

AFI 33-215, *Controlling Authorities for COMSEC Keying Material*

AFI 37-124, *The Information Collections and Reports Management Program ; Controlling Internal, Public, and InterAgency Air Force Information Collections* (will convert to AFI 33-324)

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

AFKAG-2, (FOUO) *AF COMSEC Accounting Manual*

AFKAO-5, *(C) Instructional Guide for Operations Codes* (U)

NACSIM 7001, *(C) COMSEC Planning Guide for Manual Cryptosystems* (U)

NSTISSI 3014, (FOUO) *Management of Off-Line Cryptosystems*

AFSSI 4100, *(C) Communications Security Program* (U) (will convert to AFI 33-201)

Abbreviations and Acronyms

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

COMSEC—Communications Security

DIRNSA—Director of National Security Agency

HQ AFCA—Headquarters Air Force Communications Agency

HQ CPSG—Headquarters Cryptologic Systems Group

MAJCOM—Major Command

NACSIM—National COMSEC/EMSEC Information Memorandum

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

NSA—National Security Agency

Terms

Authentication Systems—COMSEC aids having key variables and a rule which two communicating parties can use to show their friendliness toward one another. Tactical authentication systems are based on the two parties enciphering a known element (either derived from a present rule or stated in communications) and comparing the resultant cipher values. Almost everyone who communicates at the tactical level needs some means of authentication. There are two ways to authenticate in the Air Force: "challenge and reply" and "transmission." The operational distinction between the two is that the "challenge and reply" method requires two-way communications and "transmission" does not. Both methods are used to verify that a message passed on a net was originated by an authorized person or station. However, one can use "challenge and reply" to identify friend or foe if not transmitting a message.

Code—Any system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. Coding has three distinctly different applications: (1) In the broadest sense, coding is a means of converting information into a form suitable for communications or encryption (for example, coded speech, Morse code, teletypewriter codes, and so forth). No security is provided. (2) Brevity lists are codes that are used to reduce the length of time necessary to transmit information (for example, long, stereotyped sentences may be reduced to a few characters that are transmitted). No security is provided. (3) A cryptosystem in which the cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plaintext information elements that are primarily words, phrases, or sentences. Security is provided.

Evaluation—A term used to describe the process when a revalidation of a survey or a manual cryptosystem is conducted.

Manual Cryptosystems—Cryptosystems in which the cryptographic processes are performed manually without the use of cryptoequipment or auto-manual devices.

Numeral Codes—Numeral codes are among the simplest and most useful codes. As the name infers, use these codes to encode numbers. Use them to protect the intelligence-bearing aspects ("when," "where," "how many") of tactical communications (especially voice communications). Some numeral codes are actually cipher systems because they transform plain-language formations of unfixed length into characters or groups of characters of fixed length. Numeral codes (or ciphers) are normally used with a brevity list. The characters that relate to specific terms or meanings in brevity lists are encoded with numeral codes (or ciphers).

Operations Codes—Use these, in contrast to "numeral codes," to encode the intelligence-bearing aspects ("what," "who," "why," "how," and "when") of tactical communications. Unlike numeral codes, operations codes do not provide adequate protection of information if they are mixed with plain language. The interspersed plain language tends to reveal the nature of encoded meanings. Operations codes have a vocabulary, usually from 1,000 to 3,000 entries and generally use trigraph (three-letter) code groups. Operations codes are multipurpose in that you may use them to encrypt different kinds of information related to a particular operational function.

Revalidation—An examination of a manual cryptosystem, by the controlling authority, to ensure its adequacy of design and content, continued need, proper distribution, and the controlling authority are correctly identified.

Special-Purpose Codes—Similar to operations codes but, more commonly, are designed for encoding

certain specialized messages such as radar reports or personnel summaries. Their vocabularies are usually limited in size and scope, and their code groups may be either two-letter or three-letter symbols. Many special-purpose codes are of the one-time variety in which a given arrangement of code groups may be used to encrypt only one message.

Survey—A management technique whereby actual holders of manual cryptosystems express opinion on system suitability and provide usage information for technical evaluation.

Attachment 2

CHECKLIST ITEMS FOR SUBMITTING NEW CODE OR AUTHENTICATION SYSTEM REQUIREMENTS

A2.1. Table A2.1. contains a list for checking items for submitting new code or authentication system requirements:

Table A2.1. Checklist for Checking Items for Submitting New Code or Authentication System Requirements.

	Codes	Auth Sys
1. Objective. What operational needs are you satisfying?	X	X
2. General Employment:		
a. What are the echelons of intended use?	X	X
b. What type of communications system will you use (voice, teletype, etc., point-to-point, air-ground-air, etc.)?	X	X
c. Is the code or authentication system to replace one presently in use? If so, which one?	X	X
d. Have you determined that you cannot satisfy the requirement by use of:		
(1) An auto-manual (for example, KL-43) or secure voice system?		
(2) A code or authentication system already in existence? **NOTE:** Include a statement justifying use of a manual cryptosystem rather than an auto-manual or secure voice system.	X	X
e. What is the type (operational, logistical, administrative, training, and so forth) and highest classification of traffic you need to protect?	X	X
f. What are you authenticating (access, identify, message, and so forth)?		X
g. Are you securing joint, allied, and, or combined communications systems?	X	X
(1) If used jointly, have you coordinated the requirement with all parties involved? (This is usually the responsibility of the requesting command and should be accomplished before submitting this checklist.)	X	X
(2) Whenever joint or international use is planned, indicate the extent of coordination in the request.	X	X
(3) Is there a requirement for multilingual use of the system? If so, state languages. If translated version of the system and/or operating instructions is in other than English or Arabic letters and numbers are required, furnish a sample in the exact format desired.	X	X

(4) What command or activity will you designate as the controlling authority for the system (responsibility for control, implementation, supersession training, and so forth). Include telephone number and office symbol.	X	X
(5) Who will encrypt, decrypt, or authenticate (trained cryptopersonnel, message center personnel, staff, and so forth)?	X	X
3. Specific Employment:		
a. Will you use the system to secure point-to-point communications or a communications net? Provide a diagram or narrative indicating all links, units, and intercommunication as an attachment to this checklist.	X	X
b. What is the minimum acceptable speed, in words per minute, required for encryption or authentication?	X	X
c. What is the number of holders (copies) needed and how many copies, if any, are required for reserve?	X	X
d. How many of the copies will you use to originate traffic or authentications in any single period?	X	X
e. What is the average length of a message expressed in groups or characters?		X
f. What is the average number of authentications required per day? Per week?		X
g. What is the average number of messages per day or week you will encrypt?		X
h. Are there logistic problems? For instance, are some users so isolated as to preclude the use of frequently superseded material?	X	X
i. Is a provision for expansion of the number of holders (copies) on short notice required? If so, under what circumstances will you expand and how many holders will you add?	X	X
4. Vocabulary:		
a. Attach complete sample of the desired vocabulary. Consider the following in formulating any vocabulary:		
(1) Will you encrypt numbers, letters, or both?	X	
(2) Are frequently used words, numbers, or phrases indicated so that code group variants are provided?	X	
(3) Is spelling necessary? To what extent? Keep spelling to a minimum, for security reasons. The use of brevity codes or manuals, whose symbols are in turn encrypted, provide an excellent means of maintaining security and limiting time required for encryption and decryption.	X	

(4) Are spare code groups needed and, if so, how many? Indicate where needed.	X	
b. If a suitable vocabulary is contained in an existing code, cite that code. If changes to an existing code can provide a good sample of desired vocabulary, cite the code and the required changes.	X	
c. Can you prepare the message content in a standardized format? If so, provide, insofar as possible, the desired format containing all desired stereotype phrases, configurations, etc.	X	
5. Security:		
a. Are you considering a mixture of clear and encrypted text? **NOTE:** This practice will usually result in an insecure code system. Therefore, the mixture of clear and encrypted text is authorized for one-time systems only and those used solely for the encryption of numerals.	X	
b. For what length of time (hours, weeks, months, years) after encryption will transmitted information retain its classification?	X	
c. What is the desired supersession rate for the code? Normally, the volume of traffic encrypted in a code significantly affects the supersession rate. Note that one-time systems are superseded as used and provide maximum security. For this reason, consider a one-time system first when long-term security is necessary.	X	
d. What is the desired supersession rate for the authentication system? Normally, the volume of authentications originated in a system affects security and has a bearing on the supersession rate.	X	
6. Physical Characteristics:		
a. Are there size and, or weight limitations for the system?	X	X
b. Is a particular format desired? If so, specify and, or provide a sample.	X	X
c. Is a special paper or material desired for printing? If so, specify.	X	X
d. Will you use the system in poor lighting conditions and, or a cramped space? If so, specify.	X	X
7. Special Considerations:		
a. Do you need operating instructions with each copy of the system?	X	X
b. Do you need any special instructions with the system? If so, submit them and indicate whether to include all or part of them in each copy.	X	X
c. Give an approximate date the system is required. Sufficient lead-time is necessary to enable approval and acceptance of samples, production, and distribution. To preclude emergency production, a lead-time of 4 to 6 months is requested.	X	X

d. Indicate any miscellaneous or special consideration concerning the system and its use not covered above which would aid in processing the request.	X	X
8. Classification. When this checklist is completed, assign a security classification according to AFI 31-401, Managing the Information Security Program.		

Attachment 3

ITEMS FOR SURVEY CHECKLIST

A3.1. As a minimum, surveys will include the following:

A3.1.1. Description of the using organization and its mission.

A3.1.2. Description of the purpose of the system.

A3.1.3. Description of any areas where the system fails to fulfill the operational requirement and degree to which the cryptosystem fulfills the operational requirement.

A3.1.4. Statement that local regulations, operations orders, or other directives governing the system use are current and do not conflict with system operating instructions.

A3.1.5. Availability and adequacy of training materials.

A3.1.6. Verification of total copies of manual cryptosystems received by each COMSEC account and copies distributed to the users.

A3.1.7. Description of the operating environment.

A3.1.8. Identification of users by job function and type of organization.

A3.1.9. Description of the communication systems and mediums used with the systems.

A3.1.10. Number and average length of messages encrypted in the system during the survey period in order to obtain an approximation of the type of traffic and average traffic level of the messages in the system.

A3.1.11. Categories of information and formats of messages encrypted in the system during the survey period.

A3.1.12. Number of authentications transmitted or received during the survey period (authentication systems only).

A3.1.13. Classification of the information encrypted by the system.

A3.1.14. Perishability of the information encrypted by the system.

A3.1.15. Vocabulary or format revisions needed. (This should include deletion of obsolete vocabulary items as well as addition of new words and phrases.)

A3.1.16. Spare group assignments to incorporate into the vocabulary.

A3.1.17. Locally produced brevity lists or devices, if any, used with the system. (If applicable, include description or sample.)

A3.1.18. Number of locally reproduced copies, if any.

A3.1.19. Any logistical problems encountered in the use of the system.

A3.1.20. General comments concerning the system. Include satisfaction or dissatisfaction with the system, suggested changes to instructions, suggested changes to physical size, and so forth.